

## **Remarks**

### **Status of the Claims**

As acknowledged by the examiner, on January 15<sup>th</sup>, 2008 we elected the Invention of Group I (claims 1-28 and 31-43), and thereby are not claiming claims 29-30 at this time.

Claims 1-28 and 31-43 are pending in the application. All claims stand rejected. By this paper, claims 1-6,8,31,33,and 40-42 have been amended, which includes all independent claims. No new matter has been added. Reconsideration of all pending claims herein is respectfully requested.

### **Claim Rejections - 35 U.S.C. §101**

Claims 1-28 were rejected under 35 U.S.C. §101 as being non-statutory subject matter. Independent claims 1, 3, and 5, and dependent claims 2, 4, 6, and 8 have been amended to recite that the tokens are stored "in an electronic token log" so that they may subsequently be retrieved by "the computing device of the authorizing institution." The amended claims therefore require that the process be tied to a computing apparatus, thus providing for statutory subject matter. Support for these amendments can be found, for example, in Fig. 4 and Fig. 5 of the disclosure.

### **Claim Rejections - 35 U.S.C. §102**

Claims 1-10, 14-28, 31-35, and 39-45 were rejected under 35 U.S.C. §102 as being anticipated by Checchio (US PAT 6,023,682). The claims have been amended to emphasize the novelty of the claims of the present disclosure relative to Checchio.

Specifically, the independent claims have been amended to clarify that storing tokens and associating tokens with conditions in the electronic token log occurs through a communication channel that is distinct from the communication channel of the transaction authorization. For example, claim 1 as amended recites the limitation that “the vendor contacts the computing device of the authorizing institution through a communication channel that is distinct from a communication channel by which the plurality of tokens are recorded in the electronic token log.” Support for these amendments can be found, for example, in the specification at paragraph [0018] and in Figs 1, 2, and 4. Checchio does not disclose this limitation, and accordingly does not anticipate or render obvious the claims as amended.

The claim amendments clarify the relationship and interaction between the entities involved in the disclosed method. The entities involved are as follows:

- Entity B (buyer / account holder) – an entity desiring to facilitate a transaction by instigating the authorization of the transaction.
- Entity F (financial institution with the buyer's financial account) – an entity responsible for authorizing (or rejecting) the transaction.
- Entity V (vendor the buyer is purchasing from) – an entity who is the recipient of the transaction and the transaction authorization.
- Entity T (thief desiring to access the buyer's account) – an entity desiring to initiate an unauthorized transaction involving the account.

Entity B is a buyer of goods or services and entity V is a vendor (or seller); entity F is a financial institution where the buyer has an account; entity T is a thief who attempts

to initiate a transaction with a seller on the financial account of the buyer against the wishes of the buyer. The present disclosure contemplates that the financial institution F has an account identifier (e.g. credit card number) for the buyer, and possibly also an authorization code such as a personal identification number, and that the thief T has gained access to the account identifier and possibly the authorization code.

Both Checchio and the present disclosure attempt to solve a similar problem but do so in very different ways. That problem is for B to initiate a transaction involving financial account with F, resulting in F providing authorization to V, yet preventing T from receiving authorization for transactions on that account. For example, Checchio refers to B as the "user," V as the "vendor," and F as the "credit card company data base" (column 3 lines 1-30). The present disclosure refers to B as the "account holder," V as the "vendor," and F as the "authorizing institution" (see disclosure and amended claims).

The shortcoming of the Checchio invention is demonstrated by the ease with which unauthorized entities (T) can initiate transactions using information covertly obtained from B. If a thief (T) obtains the personal identification code (PIC) of a legitimate user, then the thief can easily initiate transactions involving the users account. The thief simply provides the vendor with the stolen account identifier and PIC, and the Checchio invention allows the thief to receive authorization for an unauthorized transaction with a vendor.

The claims of the present disclosure improve the ability of the transaction authorization system to discriminate among authorized and unauthorized transaction initiators, and prevents such a thief from successfully executing unauthorized

transactions. The present disclosure and the amended claims emphasize the **inventive elements** that allow B to contact F “through a communication channel that is distinct from the transaction interaction with the vendor” (V). Specification, para. [0018]. In other words, the claims recite a functional mechanism for a second communication channel that is distinct from the single communication channel described in prior art, and outlined below. When the thief (T) does not have access to the second communication channel, that thief will be unable to successfully execute unauthorized transactions.

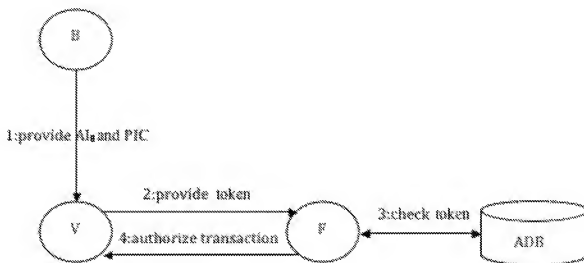
### **Single-Channel Authorization Request Systems (SCARS)**

Currently, the prior art, including Checchio, contemplates F providing B with an account identifier (e.g. a credit card number) to be used with future transactions. A request for transaction authorization proceeds as follows (Checchio Fig. 1):

1. B initiates a transaction by providing V with a credit card number and PIC.
2. V creates a token by encrypting transaction information (credit card number and purchase amount) with the PIC, and forwards the token and transaction information to F.
3. F checks the validity of the token by creating a test token by encryption using the PIC that they already have for the account as the encryption key.
4. F provides V with transaction authorization if the received token matches the test token.

These steps are diagrammed in Figure A below, where ADB is an account database maintained by F. We call this method a single-channel authorization request system (SCARS), because B requests transaction authorization solely by contacting F through V.

**Figure A:** Single-Channel Authorization Request System (e.g., Checchio invention)



The present disclosure does NOT involve the encryption steps required by Checchio. Instead, the present disclosure involves a second authorization channel, which Checchio does not consider.

### **Dual-Channel Authorization Request System (DCARS)**

The present disclosure is different from single-channel authorization request systems, and includes additional steps and system components. The inventive steps and system components allow B to request transaction authorization by contacting F through V and simultaneously allowing B to contact F by placing a Transaction

Authorization Token (TAT) in a Token Log which is accessible by F. Thus, B requests transaction authorization through two distinct channels simultaneously.

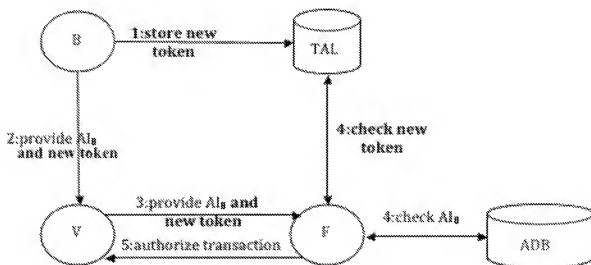
A request for transaction authorization under a dual-channel authorization request system, as was described in FIG. 1 and FIG. 2 of the present disclosure, is illustrated in Figure B below, and is emphasized in the amended claims. A transaction authorization under a dual-channel authorization request system is summarized as follows:

1. **B initiates the creation of a new TAT for storage in a Token Log accessible by F.**
2. B initiates a transaction by providing V with the account identifier **and the new TAT.**
3. V forwards the account identifier **and new TAT** to F.
4. F checks the validity of the account identifier and the status of the account **and the validity of the TAT received from V by polling the Token Log.**
5. F provides V with authorization as appropriate.

The "bolded" components in those five steps represent a technical contribution over prior art. The examiner will observe that developments of SCARS such as Checchio focus exclusively on transactions in which B requests transaction authorization from F only by communicating through V. Traditionally technologies have made it too cumbersome to have B initiate transactions by contacting F directly, which still would be prohibitive had we not provided the inventive system element of a Token Log. **For this reason, mere reconfiguration of traditional SCARS approaches**

would not lead one skilled in the art to discover the DCARS approach, and the present disclosure is therefore non-obvious.

**Figure B:** Dual-Channel Authorization Request System (corresponds to FIG. 1 and FIG. 2 of the present disclosure)



The **unexpected functional advantage** of a DCARS is that a DCARS is significantly more secure than a SCARS. As described above, under SCARS, if entity T steals the account identifier and PIC belonging to B, then entity T can present that account identifier and PIC to V in order to initiate an unauthorized authorization from F. A single-channel system simply cannot prevent such an occurrence, as demonstrated by the continued widespread identity theft as reported in the media.

By contrast, under a DCARS, entity T would not have access to the Token Log and therefore would not have access to the second channel of transaction authorization request. At step 4 of the DCARS procedure described above, entity F would not find a

valid TAT in the Token Log and would therefore reject the unauthorized transaction authorization request. This is a significant functional advantage over SCARS.

Because Checchio does not disclose the distinct communication paths recited in the claims of the present disclosure, Checchio does not anticipate or render obvious claims 1-28 and 31-43.

#### Claim Rejections – 35 USC §103

Dependent claims 11-13 and 36-38 were rejected for obviousness under 35 U.S.C. 103(a) relative to Checchio. These claims depend upon independent claims 5 and 31, which have been amended and which have been shown above to be distinct from the Checchio invention, and nonobvious. Therefore, claims 11-13 and 36-38 taken with claims 5 and 31 are nonobvious.

In summary, amended independent claims 1, 3, 5, 31, and 40-42 are patentably distinct over the prior art of record. All other claims are dependent upon one of the foregoing claims and are therefore patentably distinct for at least the same reasons. A Notice of Allowance is respectfully requested.



Respectfully submitted,

By /Kory D. Christensen/  
Attorney for Applicant  
Registration No. 43,548

STOEL RIVES LLP  
One Utah Center Suite 1100  
201 S Main Street  
Salt Lake City, UT 84111-4904  
Telephone: (801) 328-3131  
Facsimile: (801) 578-6999